Identities in modular arithmetic from reversible coherence operations

Peter M. Hines

April 29, 2013

Abstract

This paper investigates some issues arising in categorical models of reversible logic and computation. Our claim is that the structural (coherence) isomorphisms of these categorical models, although generally overlooked, have decidedly non-trivial computational content. The theory of categorical coherence is based around reversible structural operations (canonical isomorphisms) that allow for transformations between related, but distinct, mathematical structures. A number of *coherence theorems* are commonly used to treat these transformations as though they are identity maps, from which point onwards they play no part in computational models. We simply wish to point out that doing so overlooks some significant computational content.

We give a single example (taken from an uncountably infinite set of similar examples, and based on structures used in models of reversible logic and computation) of a category whose structural isomorphisms manipulate modulo classes of natural numbers. We demonstrate that the coherence properties that usually allow us to ignore these structural isomorphisms in fact correspond to countably infinite families of non-trivial identities in modular arithmetic. Further, proving the correctness of these equalities without recourse to the theory of categorical coherence appears to be a hard task.

1 Introduction

1.1 Historical background

In [6], J.-Y. Girard introduced *Linear Logic*, a striking new decomposition of classical logic. By contrast to previous approaches to logic, it was based around the twin related principles of *reversibility* and *resource-sensitivity*. Although the structural operations of copying and contraction (i.e. deletion against a copy) were not completely abandoned (as in sub-structural logics [23]), they were severely restricted. Via the Curry-Howard isomorphism [21] (also known as the 'proofs-as-programs' correspondence) linear logic also has a close connection

with reversible and resource-sensitive versions of computing systems such as lambda calculus and combinatory logic [2].

The computational interpretation was pushed further in the *Geometry of Interaction* program [9], giving related models of linear logic [7, 8] (see also [4]). Although these models were degenerate in the logical sense (they identified conjunction with disjunction, and existential quantification with universal quantification) their computational content remained, as demonstrated by a series of practical computational interpretations in [8]. (As shown later [12], the dynamical part of the Geometry of Interaction system was implemented using precisely the same tools required to model reversible (space-bounded) Turing machines).

A significant challenge for logicians at this point was to give categorical models of both Linear Logic and the (related but distinct) Geometry of Interaction system, following the close correspondence between logics / type systems, and closed categories pioneered by [17]. For the purposes of this paper, we concentrate on the more computationally oriented Geometry of Interaction.

Several authors [1, 10, 15] noted that the dynamical, or computational, part of the Geometry of Interaction system was a form of *compact closure* [16] arising from categorical constructions [15, 1] on the category of partial reversible functions. As pointed out in [10, 11, 2] (and implicit in [7]), the Geometry of Interaction is an essentially untyped (in the sense of λ-calculus) reversible computational system — this is a consequence of the requirements of reversibility and resource-sensitivity. Any categorical interpretation must take this into account.

1.2 The purpose of this paper

The purpose of this paper is simply to point out some previously overlooked, decidedly non-trivial, computational content that arises in these models (in fact, familiarity with the logical models and computational systems listed above is not a requirement for understanding this paper – but does help place the theory firmly within its historical context). The computational content comes, not from the dynamics of the GoI system (i.e. compact closure in categories of partial reversible functions), but simply from the fact that the system in question is untyped. Categorically, a model of an untyped system is a category with precisely one object (i.e. a monoid). Thus the GoI system is modelled within a monoid of partial reversible functions.

In categorical logic / categorical models of computation, it is standard to ignore completely a class of structural isomorphisms known as *coherence isomorphisms*. There is a formal justification for doing so — any category with non-trivial structural isomorphisms is equivalent (in a very precise sense) to one with trivial structural isomorphisms [22].

However, there is a subtlety that is often overlooked; the process of constructing this equivalent category with trivial structural isomorphisms involves modifying the collection of objects of the category (& hence, by the correspondence between categories and logics pioneered in [17], modifying the type

system). An appendix to [14] (see also [13]) makes clear what this means for untyped systems; the 'equivalent' version with trivial structural isomorphisms has a countably infinite class of objects, and thus is no longer type-free.

As type-freeness is such an essential component of the GoI system, we are thus forced to deal with these structural isomorphisms – this paper studies a set of such isomorphisms that arise implicitly in [7]. We demonstrate that, although the category itself has only one object, modulo classes of integers play the same rôle as objects in this untyped setting. Thus, the structural isomorphisms correspond to (highly non-trivial) identities in modular arithmetic. Further, the classic theory of coherence that usually allows us to ignore structural isomorphisms completely in this case allows us to derive infinite sets of identities in modular arithmetic, essentially for free.

1.3 Categorical identities up to isomorphism

In category theory, especially the theory of monoidal categories, *coherence isomorphisms* are reversible structural operations that transform objects of categories (frequently, concrete mathematical structures) into isomorphic objects that differ only by a simple structural equivalence.

The canonical example, of course, is *associativity*, where for foundational reasons one must replace the strict identity $X \otimes (Y \otimes Z) = (X \otimes Y) \otimes Z$ by a pair of mututally inverse isomorphisms

$$X \otimes (Y \otimes Z) \underset{\tau^{-1}_{X,Y,Z}}{\overset{\tau_{X,Y,Z}}{\rightleftarrows}} (X \otimes Y) \otimes Z$$

These natural isomorphisms are required to satisfy a family of *coherence conditions* that ensure that any such re-bracketing is both reversible and confluent.

The distinction between a strict structural property (based on equality) and one that holds up to isomorphism is subtle, and a variety of coherence theorems [22] tell us that for all practical purposes, we may ignore this subtlety, and treat properties such as associativity as though they are strict. However, a passing comment in the appendix of [14] (expanded upon in a talk given by the author at Dagstuhl Seminar 12352, 'Information Flow and its Applications' [3]) observes that in various settings, these structural isomorphisms are concrete reversible arithmetic operations and the very coherence theorems used to ignore them have non-trivial computational content.

This paper expands upon these observations via a simple representative example. We give an untyped (i.e. single-object) unitless monoidal category whose structural isomorphisms are based on modular arithmetic, and then describe the significant computational advantage that the theory of categorical coherence provides in decisions procedures for equality of such reversible operations. In particular, we demonstrate that categorical diagrams based on k distinct nodes correspond to arithmetic identities over equivalence classes of the form $\{2^k.\mathbb{N} + x\}_{x=0\ldots 2^k-1}$. Despite this, the coherence theorem for associativity

provides, for free, a large (countably infinite) class of arithmetic identities over such modular clases that are guaranteed to be correct. At least to the author, these identities are not readily apparent simply from their algebraic description.

1.4 MacLane's coherence theorem for associativity, and untyped monoidal categories

MacLane's coherence theorem for associativity is commonly, although incorrectly, described as stating that 'all diagrams built from coherence isomorphisms commute'. This is a correct characterisation of the more technical result in some, but certainly not all, cases (in particular simple calculations will demonstrate that it does not hold the for constructions of this paper). The distinction becomes important when the objects of the category do not satisfy a 'freeness' condition with respect to the monoidal tensor, leading to what [22] refers to as *undesirable identifications between objects*. Thus, when the class of objects is not only a set, but is *finite*, the informal characterisation above can never coincide with the formal statement of the theorem.

This paper presents a rather extreme example of this: we exhibit a small (unitless) symmetric monoidal category with exactly one object N satisfying the equality[1] $N \otimes N = N$, as in the example of J. Isbell used by MacLane to motivate the notion of coherence up to isomorphism [22] p. 160.

This 'untyped' monoidal category is an example of a general construction introduced in [10, 11] – see also [14, 13]. As demonstrated in an Appendix to [14], there are uncountably many such untyped monoidal categories based on functions on $\mathbb{N}$ (in 1:1 correspondence with the interior points of the Cantor set, excluding a subset of measure zero), of which the one we present is merely the simplest.

We then describe which canonical diagrams of this category are predicted to commute by MacLane's coherence theorem for associativity, and demonstrate that these are non-obvious identities in modular arithmetic.

2 An untyped monoidal category

We first give some simple arithmetic constructions on $\mathbb{N}$, based on arithmetic modulo 2^k, for $k \in \mathbb{N}$, with a close connection to the theory of symmetric monoidal categories [22]:

Definition 2.1. *Let us denote the monoid of bijections on the natural numbers by $\mathcal{J}$, and treat this as a single-object category. We define $\tau, \sigma \in \mathcal{J} = \mathcal{J}(\mathbb{N}, \mathbb{N})$*

[1] Note that this is strict equality, rather than isomorphism. For category-theorists worried about foundational questions related to a notion of equality between objects, we emphasise that this is a *small* category. Although $N \otimes (N \otimes N) = (N \otimes N) \otimes N$, this equality of objects does not imply that the corresponding associativity isomorphism is a strict identity.

as follows:

$$\tau(n) = \begin{cases} 2n & n \ (mod\ 2) = 0, \\ n+1 & n \ (mod\ 4) = 1, \\ \frac{n-1}{2} & n \ (mod\ 4) = 3. \end{cases}$$

$$\sigma(n) \ = \ \begin{cases} n+1 & n \text{ even}, \\ n-1 & n \text{ odd}. \end{cases}$$

We also give an operation that, given two bijections on $\mathbb{N}$*, returns another bijection. Given arbitrary* $f, g \in \mathcal{J}$*, we define*

$$(f \star g)(n) \ = \ \begin{cases} 2.f\left(\frac{n}{2}\right) & n \text{ even}, \\ 2.g\left(\frac{n-1}{2}\right)+1 & n \text{ odd}. \end{cases}$$

The following properties of the above bijections and operations will be established via basic modular arithmetic. These properties are, as will be apparent, closely related to the structural properties and coherence conditions of symmetric monoidal categories:

Proposition 2.2. *Let* $(\_ \star \_), \sigma, \tau$ *be as in Definition 2.1 above. Then for all* $f, g, h \in \mathcal{J}$*, the following properties hold:*

1. **Identities** $id \star id = id$
2. **Interchange** $(h \star k)(f \star g) = (hf \star kg)$
3. **Natural associativity** $\tau(f \star (g \star h)) = ((f \star g) \star h)\tau$
4. **Natural symmetry** $\sigma(g \star f) = (f \star g)\sigma$
5. **Pentagon** $\tau^2 = (\tau \star id)\tau(id \star \tau)$
6. **Hexagon** $\tau\sigma\tau = (\sigma \star id)\tau(id \star \sigma)$

Proof.

1. By definition, $(id \star id)(n) = \begin{cases} 2\left(\frac{n}{2}\right) \ = \ n & n \text{ even}, \\ 2\left(\frac{n-1}{2}\right)+1 \ = \ n & n \text{ odd}. \end{cases}$
2. Similarly, $(h \star k)(f \star g)(n) = \begin{cases} (h \star k)\left(2f\left(\frac{n}{2}\right)\right) & n \text{ even}, \\ (h \star k)\left(2g\left(\frac{n-1}{2}\right)+1\right) & n \text{ odd}. \end{cases}$

   Now observe that $2f\left(\frac{n}{2}\right)$ is always even, for arbitrary choice of $f \in \mathbf{Bij}(\mathbb{N}, \mathbb{N})$ and even $n \in \mathbb{N}$. Similarly, $2g\left(\frac{n-1}{2}\right)+1$ is always odd, for arbitrary choice of $g \in \mathbf{Bij}(\mathbb{N}, \mathbb{N})$ and odd $n \in \mathbb{N}$. Thus

$$(h \star k)\left((f \star g)(n)\right) = \begin{cases} 2h\left(\frac{2f\left(\frac{n}{2}\right)}{2}\right) & n \text{ even}, \\ 2k\left(\frac{\left(2g\left(\frac{n-1}{2}\right)+1\right)-1}{2}\right)+1 & n \text{ odd}. \end{cases}$$

Simplifying this expression,

$$(h \star k)(f \star g)(n) = (hf \star kg)(n) = \begin{cases} 2hf\left(\frac{n}{2}\right) & n \text{ even}, \\ 2kg\left(\frac{n-1}{2}\right) + 1 & n \text{ odd}. \end{cases}$$

3. We first establish explicit formulæ for $f \star (g \star h)$ and $(f \star g) \star h$. By definition,

$$(f \star (g \star h))(n) = \begin{cases} 2f\left(\frac{n}{2}\right) & n \text{ even}, \\ (g \star h)\left(\frac{n-1}{2}\right) + 1 & n \text{ odd}. \end{cases}$$

Unwinding the definition of $(g \star h)$,

$$(g \star h)\left(\frac{n-1}{2}\right) = \begin{cases} 2g\left(\frac{n-1}{4}\right) & \frac{n-1}{2} \text{ even}, \\ 2h\left(\frac{\left(\frac{n-1}{2}\right)-1}{2}\right) + 1 & \frac{n-1}{2} \text{ odd}. \end{cases}$$

Thus

$$(f \star (g \star h))(n) = \begin{cases} 2f\left(\frac{n}{2}\right) & n \ (mod\ 2) \ = \ 0, \\ 2g\left(\frac{n-1}{4}\right) + 1 & n \ (mod\ 4) \ = \ 1, \\ 2h\left(\frac{n-3}{4}\right) + 3 & n \ (mod\ 4) \ = \ 3. \end{cases}$$

Using similar reasoning,

$$((f \star g) \star h)(n) = \begin{cases} 4f\left(\frac{n}{4}\right) & n \ (mod\ 4) \ = \ 0 \\ 4g\left(\frac{n-2}{4}\right) + 2 & n \ (mod\ 4) \ = \ 2 \\ 2h\left(\frac{n-1}{2}\right) + 1 & n \ (mod\ 2) \ = \ 1 \end{cases}$$

From the explicit description of τ,

$$\tau(f \star (g \star h)) = \begin{cases} 4f\left(\frac{n}{2}\right) & n \ (mod\ 2) \ = \ 0 \\ 4g\left(\frac{n-1}{4}\right) + 2 & n \ (mod\ 4) \ = \ 1 \\ 2h\left(\frac{n-3}{4}\right) + 1 & n \ (mod\ 4) \ = \ 3 \end{cases}$$

and an almost identical calculation will verify that $((f \star g) \star h)\tau$ is given by the same formula.

4. Direct calculation gives that

$$\sigma(g \star f)(n) = (f \star g)\sigma(n) = \begin{cases} 2f\left(\frac{n}{2}\right) + 1 & n \ (mod\ 2) = 0 \\ 2g\left(\frac{n-1}{2}\right) & n \ (mod\ 2) = 1 \end{cases}$$

5. We first describe the individual parts of the Pentagon equation:

$$(id \star \tau)(n) = \begin{cases} n & n \ (mod\ 2) \ = \ 0 \\ 2n-1 & n \ (mod\ 4) \ = \ 1 \\ n+2 & n \ (mod\ 8) \ = \ 3 \\ \frac{n-1}{2} & n \ (mod\ 8) \ = \ 7 \end{cases}$$

Similarly,

$$(\tau \star id)(n) = \begin{cases} 2n & n \ (mod\ 4) \ = \ 0 \\ n+2 & n \ (mod\ 8) \ = \ 2 \\ \frac{n+1}{2} & n \ (mod\ 8) \ = \ 6 \\ n & n \ (mod\ 2) \ = \ 1 \end{cases}$$

Composing, on a case-by-case basis, gives

$$\tau^2(n) = (\tau \star id)\tau(id \star \tau)(n) = \begin{cases} 4n & n \ (mod\ 2) \ = \ 0 \\ n+2 & n \ (mod\ 4) \ = \ 1 \\ \frac{n+1}{2} & n \ (mod\ 8) \ = \ 3 \\ \frac{n-3}{4} & n \ (mod\ 8) \ = \ 7 \end{cases}$$

6. For the hexagon equation, direct calculations (that by this stage, we are happy to leave as an exercise) demonstrate that

$$\tau\sigma\tau(n) = (\sigma \star id)\tau(id \star \sigma)(n) = \begin{cases} 2n+2 & n \ (mod\ 2) \ = \ 0 \\ \frac{n+1}{2} & n \ (mod\ 4) \ = \ 1 \\ n-3 & n \ (mod\ 4) \ = \ 3 \end{cases}$$

□

Remark 2.3. *$\mathcal{J}$ is a monoid — a one-object, or single-typed, category. Despite this, the above calculations demonstrate how the rôle of distinct objects in the theory of symmetric monoidal categories is instead played by certain subsets of $\mathbb{N}$ — the congruence classes of the form $\{2^k.\mathbb{N} + x\}_{x=0\ldots 2^k-1}$.*

As demonstrated in Proposition 2.2 above, $(\mathcal{J}, \star, \tau, \sigma)$ has all the structure of a symmetric monoidal category, except for the existence of a unit object. We axiomatise such situations as follows:

Definition 2.4. *Let $\mathcal{C}$ be a category. We say that $\mathcal{C}$ is* **semi-monoidal** *when it satisfies all the properties for a monoidal category except for the requirement of a unit object — i.e. there exists a* **tensor** $(\ \Box\ ) : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ *together with a natural object-indexed family of* **associativity isomorphisms** $\{\tau_{A,B,C} : A\Box(B\Box C) \to (A\Box B)\Box C\}_{A,B,C \in Ob(\mathcal{C})}$ *satisfying MacLane's pentagon condition*

$$(\tau_{A,B,C}\Box 1_D)\tau_{A,B\Box C,D}(1_A\Box\tau_{B,C,D}) \ = \ \tau_{A\Box B,C,D}\tau_{A,B,C\Box D}$$

When there also exists a natural object-indexed natural family of **symmetry isomorphisms** $\{\sigma_{X,Y} : X\Box Y \to Y\Box X\}_{X,Y \in Ob(\mathcal{C})}$ *satisfying MacLane's hexagon condition*

$$\tau_{A,B,C}\sigma_{A\Box B,C}\tau_{A,B,C} \ = \ (\sigma_{A,C}\Box 1_B)\tau_{A,C,B}(1_A\Box\sigma_{B,C})$$

we say that $(\mathcal{C}, \Box, \tau, \sigma)$ is a **symmetric semi-monoidal category**.

A functor $\Gamma : \mathcal{C} \to \mathcal{D}$ between two semi-monoidal categories $(\mathcal{C}, \Box_{\mathcal{C}})$ and $(\mathcal{D}, \Box_{\mathcal{D}})$ is called (strictly) **semi-monoidal** *when $\Gamma(f\Box_{\mathcal{C}}g) = \Gamma(f)\Box_{\mathcal{D}}\Gamma(g)$. All monoidal categories are semi-monoidal, but not vice versa; the relationship is*

precisely analogous to that between monoids and semigroups. When a semi-monoidal category does not contain a unit object, we call it **unitless monoidal**.

When a semi-monoidal category has only one object, we call it **untyped monoidal**, *or simply* **untyped**.

Theorem 2.5. *The structure* $(\mathcal{J}, \_ \star \_, \tau, \sigma)$, *as given in Definition 2.1 is an untyped symmetric monoidal category.*

Proof. This follows from Proposition 2.2 above. □

Remark 2.6. *As observed in [14], we may construct similar structures based on congruence classes of the form* $\{p^k\mathbb{N} + x\}_{x=0\ldots p^k-1}$, *for arbitrary* $p \geq 2 \in \mathbb{N}$, *and in general the untyped symmetric monoidal structures on the monoid of bijections on the natural numbers are in 1:1 correspondence with the interior points of the Cantor set (and thus are uncountably infinite). We also refer to [10, 18] for many examples of these, given in terms of algebraic representations of inverse semigroups. As observed in the introduction, these are heavily used in models of reversible computation and logic.*

2.1 Coherence in unitless monoidal categories

When working with semi-monoidal categories, it would be exceedingly useful to be able to rely on MacLane's coherence theorems, for both associativity and (when appropriate) symmetry. A natural worry, therefore, is whether there is some exceedingly subtle interaction between the existence of a unit object, and the monoidal tensor, that means these theorems are not applicable in the absence of a unit object.

Readers familiar with the proof of MacLane's coherence theorem for associativity will recall that associativity and the units conditions are treated individually, and so this is unlikely to be the case. A conclusive argument is provided by an Appendix to [13], where the obvious procedure for adjoining a (strict) unit object to a semi-monoidal category is described, and proved to be adjoint to the equally obvious forgetful functor. Thus, a semi-monoidal category may be transformed into a monoidal category with no side-effects.

Despite this, there is a subtlety about *untyped* monoidal categories that is worth observing. In [22], MacLane gives an argument, due to J. Isbell, for considering associativity up to canonical isomorphism, rather than up to strict identity. This argument was based on a denumerable object D in the skeletal category of sets satisfying $D \otimes D = D$, and a proof that strict associativity at this object would force a collapse to a triviality (i.e. the unit object for this category). Isbell's argument was phrased in terms of a single category with categorical products — an appendix to [14] argues that this is the case in arbitrary untyped monoidal categories, and a full coherence result is given in [13].

2.2 Coherence in the untyped monoidal category $(\mathcal{J}, \star)$

In Section 2.1, we have seen that canonical isomorphisms for the untyped monoidal category $(\mathcal{J}, \star)$ are simply arithmetic expressions, built using modular arithmetic. Thus, it is possible (albeit frequently tedious and complex – see also Section 3) to verify whether or not a diagram commutes by direct calculation. Fortunately, we are also able to use MacLane's coherence theorem for associativity to derive — from basic categorical principles — a large class of diagrams that are guaranteed to commute, and thus a large class of number-theoretic identities that are guaranteed to be true.

However, we are not able to use the common simplification of the associativity theorem — valid in a wide range of settings — that states *all canonical diagrams commute*. Since all arrows of $\mathcal{J}$ have the same source and target, this would imply that all arrows built recursively from the set $\left\{\tau, (\_ \star \_), (\ )^{-1}\right\}$ are equal, and this is clearly not the case! Instead, we must use the full statement of MacLane's theorem, in order to give a large class of diagrams that are guaranteed to commute.

The coherence theorem for associativity is based on the free monogenic monoidal category. As we are interested in the unitless case, we work with this category, with the unit removed. Readers unhappy with this are invited to adjoin a unit object to $\mathcal{J}$, apply the coherence theorem for associativity, and then remove the unit object.

Definition 2.7. *We define $(\mathcal{W}, \square)$, the* **free monogenic semi-monoidal category***, to be precisely MacLane's free monogenic monoidal category [22], with the unit object removed. An explicit description follows:,*

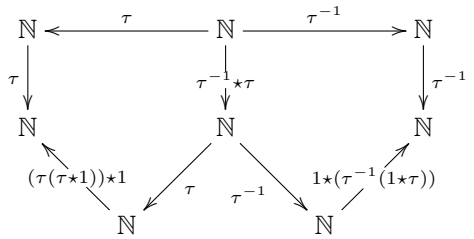
- *(***Objects***)* *These are non-empty binary trees over a single variable symbol x. Thus, $x \in Ob(\mathcal{W})$, and, for all $a, b \in Ob(\mathcal{W})$, the formal string $a \square b \in Ob(\mathcal{W})$.*
- *(***Arrows***)* *Given $w \in Ob(\mathcal{W})$, the* **rank** *of w is the number of occurrences of the symbol x within the string w, so $rank(x) = 1$, and $rank(w) \geq 1$ for arbitrary $w \in Ob(\mathcal{W})$. There then exists a unique arrow between any two objects a, b of the same rank, which we denote $(b \leftarrow a) \in \mathcal{W}(a, b)$.*
- **(Composition)** *The composite of two unique arrows is simply the unique arrow with the appropriate source / target. Thus, $(c \leftarrow b)(b \leftarrow a) = (c \leftarrow a)$.*
- **(Tensor)** *On objects, the tensor of a and b is the formal string $a \square b$. The definition on arrows must then be $(b, a) \square (v, u) = (b \square v, a \square u)$.*
- **(Associativity isomorphisms)** *The canonical isomorphism from $a \square (b \square c)$ to $(a \square b) \square c$ is the unique arrow between these two objects.*

The arrows between objects of rank n correspond to the rebracketings of binary trees with n leaves, in the obvious way.

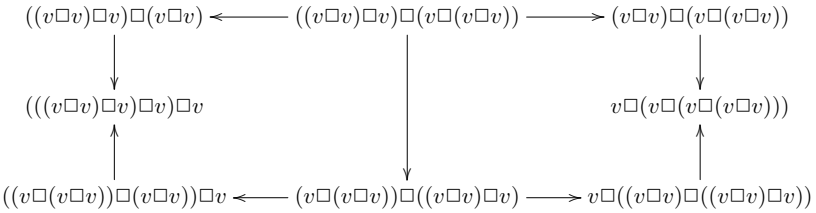
There is then a natural semi-monoidal functor, $Sub : (\mathcal{W}, \Box) \to (\mathcal{J}, \star)$, the (unitless version of the) *Substitution functor* of [22] p. 162. Expanding out the abstract definition gives the following characterisation of this functor:

- $Sub(w) = \mathbb{N}$, for all $w \in Ob(\mathcal{W})$.
- $Sub(w \leftarrow w) = id_{\mathbb{N}}$
- $Sub(a \Box v \leftarrow a \Box u) = id_{\mathbb{N}} \star Sub(v \leftarrow u)$
- $Sub(v \Box a \leftarrow u \Box a) = Sub(v \leftarrow u) \star id_{\mathbb{N}}$
- $Sub(a \Box b) \Box c \leftarrow a \Box (b \Box c) = \tau$.

MacLane's theorem states that $Sub(\mathcal{W}, \Box) \to (\mathcal{J}, \star)$ is indeed a (semi-) monoidal functor, and thus any diagram over $(\mathcal{J}, \star)$ that is the image of a diagram over $(\mathcal{W}, \Box)$ under this functor is guaranteed to commute. This simple result gives a countably infinite set of diagrams that are guaranteed to commute (and thus a corresponding set of arithmetic identities that are guaranteed to hold). For example, in $(\mathcal{J}, \star, \tau)$, the following diagram commutes:



To prove that this commutes, simply note that it is the image of the following diagram over $(\mathcal{W}, \Box)$



(We do not label the arrows of this diagram, since they are uniquely determined by their source and target. They may, of course, simply be thought of as re-bracketings of binary trees of rank 6).

3 Number-theoretic identities via coherence

We have shown that MacLane's coherence theorem provides a countably infinite set of categorical diagrams that may be guaranteed to commute; however, the basic building blocks of these diagrams are the modular arithmetic operations of

Definition 2.1 — thus the coherence theorem predicts identities within modular arithmetic. It is of course possible to verify that such diagrams, such as the above diagram, commute, using modular arithmetic and a case-by-case analysis, as in Section 2.1. However, to prove the following identities

$$\tau^2 = ((\tau(\tau \star 1)) \star 1)\tau(\tau^{-1} \star \tau) \text{ and } \tau^{-2} = (1 \star (\tau^{-1}(1 \star \tau^{-1})))\tau^{-1}(\tau^{-1} \star \tau)$$

as expressed by this diagram, would involve working with a case-by-case analysis of modulo classes of the form $\{n \ (mod\ 32) = k\}_{k=0\ldots31}$. The unfortunate referee assigned the task of verifying the calculations of Proposition 2.2 will agree that this is a task to be avoided, if at all possible.

In general, a canonical diagram with N nodes may be the image of a diagram in $(\mathcal{W}, \Box)$ containing trees of depth N. An arithmetic check of the validity of this diagram may therefore require a case-by-case analysis that includes modulo classes $\{\mathbb{N} + x \ (mod\ K)\}_{x=0\ldots K}$, where $0 \leq K < 2^N$. Clearly this is unfeasible, even for moderately large N. However, when a diagram is indeed the image of a diagram in $(\mathcal{W}, \Box)$ the coherence theorem for associativity allows us to assert equality between all paths within the diagram that have the same source and target — and thus the correctness of the (somewhat complicated) corresponding arithmetic identities.

Checking that an arbitrary diagram is within the image of this functor (and thus commutes) may be seen intuitively to be a much simpler task. In Section 4 below, we suggest that this task is in fact *linear*, instead of *exponential*.

Remark 3.1. *As well as the modular arithmetic identities predicted by the coherence theorem for associativity, it may be observed that* $(\mathcal{J}, \star)$ *is a* symmetric *untyped monoidal category, and thus the theory of coherence of symmetry will predict an additional countably infinite set of identities. This is indeed correct, and coherence for other categorical properties (e.g. the distributivity of* $\times$ *over* $\uplus$*) also provide further sets of arithmetic identities. The study of these is work in progress.*

4 Conclusions and future work

We have demonstrated that, working within a simple representative arithmetic example, MacLane's coherence theorem predicts the correctness of a countably infinite set of identities in modular arithmetic. As observed in the introduction, this particular category is simply the simplest possible example of an uncountably infinite set of similar untyped monoidal categories based on reversible arithmetic functions of the natural numbers. Thus, there appears to be considerable scope for deriving arithmetic and number-theoretic identities from categorical first principles.

Of equal interest – both in the category we give, or in any similar category — is whether we can go in the opposite direction; given a canonical diagram expressing some identities of modular arithmetic, is there a partial or complete decision procedure that will tell us whether it is the image of some diagram under MacLane's substitution functor (and thus whether the arithmetic identities

expressed are correct)? We conjecture that not only is this the case, but that the complexity of this decision procedure is linear in the number of edges of the diagram (this conjecture is based on an algorithm presented by the author at the conference [3], based on Robinson's unification algorithm [5]).

We also expect to find further applications in a number of other fields. In particular, constructions similar to those of this paper were used in an algebraic setting to give full concrete representations of Thompson's V and F groups [19, 20]. Thus, any results or decision procedures for the abstract categorical theory can reasonably be expected to find applications to the theory of these groups.

References

[1] S. Abramsky. Retracing some paths in process algebra. In *CONCUR 96*, pages 1–17. Springer-Verlag Lecture Notes in Computer Science, 1996.

[2] S. Abramsky, E. Haghverdi, and P. Scott. Geometry of interaction and linear combinatory algebras. *Mathematical Structures in Computer Science*, 12 (5), 2002.

[3] Samson Abramsky, Jean Krivine, and Michael W. Mislove. Information Flow and Its Applications (Dagstuhl Seminar 12352). *Dagstuhl Reports*, 2(8):99–112, 2013.

[4] V. Danos and L. Regnier. Local and asynchronous beta reduction. In *Proceedings of the Eighth Annual IEEE Symp. on Logic in Computer Science*, 1993.

[5] J. Gallier. *Logic for Computer Science*. J. Wiley & sons, 1987.

[6] J.-Y. Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[7] J.-Y. Girard. Geometry of interaction 1. In *Proceedings Logic Colloquium 88*, pages 221–260. North-Holland, 1989.

[8] J.-Y. Girard. Geometry of interaction ii. In *Proceedings COLOG 88*, Springer LNCS, pages 76–93. Martin-Lof & Mints, 1989.

[9] J.-Y. Girard. Toward a geometry of interaction. *Contemporary Mathematics*, 92:69–108, 1989.

[10] P. Hines. *The algebra of self-similarity and its applications*. PhD thesis, University of Wales, Bangor, 1997.

[11] P. Hines. The categorical theory of self-similarity. *Theory and Applications of Categories*, 6:33–46, 1999.

[12] P. Hines. A categorical framework for finite state machines. *Mathematical Structures in Computer Science*, 13:451–480, 2003.

[13] P. Hines. Coherence in hilbert's hotel. *arXiv:1304.5954 [math.CT]*, 2013.

[14] P. Hines. Types and forgetfulness in categorical linguistics and quantum mechanics. In M. Sadrzadeh C. Heunen, editor, *Categorical Information flow in Physics and Linguistics*, pages 215–248. Oxford University Press, 2013.

[15] A. Joyal, R. Street, and D. Verity. Traced monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, pages 425–446, 1996.

[16] M. Kelly and M. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[17] J. Lambek and P. Scott. *Introduction to Higher Order Categorical Logic*. Cambridge University Press, 1986.

[18] M. V. Lawson. *Inverse semigroups: the theory of partial symmetries*. World Scientific, Singapore, 1998.

[19] M. V. Lawson. Representations of the thompson group f via representations of the polycyclic monoid on two generators. 2004.

[20] M. V. Lawson. Orthogonal completions of the polycyclic monoids. *Communications in Algebra*, 35 (5), 2007.

[21] P. Urzyczyn M. Sørensen. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier Science, 1998.

[22] S. MacLane. *Categories for the working mathematician*. Springer-Verlag, New York, second edition, 1998.

[23] F. Paoli. *Substructural Logics: A Primer*. Kluwer, 2002.